

**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION**

ZOHO CORPORATION,

§

Plaintiff,

§

V.

§

Civil Action No. 1:22-cv-37-LY

## LIBERTY PEAK VENTURES, LLC,

§

**Defendant.**

§

## LIBERTY PEAK VENTURES, LLC,

§

## Counterclaimant,

§

V.

§

ZOHO CORPORATION,

§

## Counter-Defendant,

§

and

§

ZOHO CORPORATION PVT. LTD.

§

## Third-Party Defendant.

§

**DECLARATION OF MARKUS JAKOBSSON  
REGARDING CLAIM CONSTRUCTION**

## **INTRODUCTION**

I, Markus Jakobsson, declare as follows:

1. I submit this Declaration in support of the claim constructions positions and the opening claim construction brief of Zoho Corporation and Zoho Corporation Pvt., Ltd. (collectively “Zoho”). In particular, I submit this Declaration to provide relevant background information regarding the technology at issue in the Patents-in-Suit: U.S. Patent No. 9,373,122 (“122 patent”), U.S. Patent No. 10,074,088 (“088 patent”), and U.S. Patent No. 10,956,901 (“901 patent”) and to set forth my opinions about the meaning of certain disputed claim terms from the perspective of a person of ordinary skill in the pertinent field.

### **I. QUALIFICATIONS, EXPERIENCE, AND PUBLICATIONS**

2. The following is a brief summary of my background and qualifications. My background and qualifications are more fully set out in my curriculum vitae, which is attached as Appendix A.

3. I have at least 25 years’ experience with web-based commerce, encryption, and security systems. I am currently the Chief Scientist at Artema Labs, a crypto company I co-founded in 2021. At Artema Labs, I am responsible for the research group, which consists of seven members. My work primarily involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches; as well as coordinating and guiding the efforts of the research group. I have previously been retained as an expert witness in over 50 cases.

4. Prior to Artema Labs, my recent positions include positions at ByteDance and Amber Solutions; I was the Chief Scientist at ByteDance, the company that owns TikTok. My responsibilities included identifying security risks and improvement thereto, and to develop better technology related to ByteDance’s and TikTok’s business.

5. I was the Chief of Security and Data Analytics at Amber Solutions, Inc., a cybersecurity company that develops home and office automation technology. At Amber Solutions, my research focused on identifying and blocking abuse, including social engineering, malware and privacy intrusions.

6. I received a Master of Science degree in Computer Engineering from the Lund Instituted of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a Researcher at the San Diego Supercomputer Center, where I did research on authentication and privacy.

7. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract exchange, digital commerce including crypto payments, and fraud detection and prevention. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems, as well as improved privacy-enhancing technologies based on public key and hybrid encryption. During that time, I also predicted the rise of what later became known as phishing and developed authentication technologies to address this and other threats. I was also an Adjunct Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols.

8. From 2004 to 2016, I held a faculty position at Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for

Applied Cybersecurity Research (CACR) from 2004 to 2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, as well as e-commerce and authentication, resulting in over 50 publications and two books. Among other efforts, I supervised Dr. Sid Stamm, whose PhD thesis focused on improving browser security. I guided Dr. Stamm's research and Dr Stamm and I published extensively on topics including browser security, encryption, and e-commerce.

9. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, and Chief Scientist at Agari from 2016 to 2018. Agari is a cybersecurity company that develops and commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing countermeasures, including technological countermeasures, user interaction and education.

10. I have founded or co-founded several successful computer security companies. In 2005 I founded RavenWhite Security Inc., a provider of authentication solutions, and I am currently its Chief Technical Officer. In 2007 I founded Extricatus LLC, one of the first companies to address consumer security education. In 2009 I founded FatSkunk Inc., a provider

of mobile malware detection software; I served as Chief Technical Officer of FatSkunk from 2009 to 2013, when FatSkunk was acquired by Qualcomm and I became a Qualcomm employee. In 2013 I founded ZapFraud Inc., a provider of anti-scam technology addressing Business Email Compromise, and I am currently its Chief Technical Officer. In 2014 I founded RightQuestion LLC, a security consulting company. In 2022, I founded CSExpert LLC, a security consulting company; Carbyne LLC, a biometrics and security company; and SecurityInnovation LLC, an Internet security company.

11. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of the technical advisory board at Stealth Security (an anti-fraud company). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

12. I have authored seven books and over 150 peer-reviewed publications, and have been a named inventor on over 300 patents and patent applications. A complete list of my publications is contained in my curriculum vitae, a copy of which is attached as Appendix A to this Declaration.

13. My work has included research in the area of applied security, privacy, e-commerce, cryptographic protocols, authentication, malware, social engineering, usability and fraud. I have authored numerous publications regarding Internet security, including Internet security as it pertains to web browsers. Relevant examples include:

- “Web Camouflage: Protecting Your Clients from Browser-Sniffing Attacks,” 5 IEEE Security & Privacy (Nov. 2007)

- “Invasive Browser Sniffing and Countermeasures,” Conference: 15th International Conference on World Wide Web (May 2006)
- “Remote Harm-Diagnostics”, (PDF) Privacy-preserving history mining for web browsers (researchgate.net)
- “Privacy-Preserving History Mining for Web Browsers”, (PDF) Privacy-preserving history mining for web browsers (researchgate.net)
- “Server-Side Detection of Malware Infection”, NSPW Proceedings on New Security Paradigms Workshop (2009), Proceedings of the 2009 workshop on New security paradigms workshop (acm.org)

14. Based upon my knowledge and experience in this field, I am aware of the needs and the challenges that are and were faced by system designers in the field of internet commerce and web-based security systems, including around the 2008-2009 timeframe. This includes knowledge of systems, technologies, and techniques commonly used for securing information exchanged between browsers and servers, encryption protocols and systems that were commonly known and used at the time, and the structure and operation of web browsers and browser add-ons such as plugins and toolbars. I believe that I am considered to be an expert in these areas, and I consider myself to be an expert in these areas.

## **II. COMPENSATION**

15. I am being compensated for my time spent on this matter at my usual and customary rate of \$775 per hour. My compensation is not related to the outcome of this action and I have no financial or other commercial interest on the outcome of this case.

## **III. MATERIALS CONSIDERED**

16. In preparing this declaration, I have considered the disclosures of the Patents-in-Suit, the prosecution histories for the Patents-in-Suit and the parties’ claim construction disclosures as of the date of this declaration. I have also relied upon my years of experience in

the field, though the testimony I offer is from the person of ordinary skill as I have defined it below.

#### IV. SUMMARY OF OPINIONS

17. I understand that Liberty Peak Ventures, LLC (“LPV”) alleges that the Zoho defendants infringe the following claims:

- Claims 1, 2, 3, 5, 6, 7, 15, 16, 17, and 20 of the ’122 Patent,
- Claims 1, 5, 6, 15, 19, and 20 of the ’088 Patent, and
- Claims 1, 4, 8, 9, 11, 14, 16, 17, 18, and 19 of the ’901 Patent.

18. If called as a witness to testify at a claim construction hearing, I expect to testify on the following topics and provide opinions and testimony on what is summarized in this declaration:

- The ’122 Patent, its specification, claims, and the science underlying what is disclosed in it.
- The level of ordinary skill in the art to which the ’122 Patent is directed.
- The ’088 Patent, its specification, claims, and the science underlying what is disclosed in it.
- The level of ordinary skill in the art to which the ’088 Patent is directed.
- The ’901 Patent, its specification, claims, and the science underlying what is disclosed in it.
- The level of ordinary skill in the art to which the ’901 Patent is directed.
- My opinions on how the disputed terms identified in section **Error! Reference source not found.** below would have been interpreted by a person of ordinary skill in the art at the time of invention.
- My opinions that the Patents-in-Suit fail to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

19. In my opinion, the term “securely storing, by the browser toolbar, the account information at the browser toolbar” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

20. In my opinion, the term “securely storing the account information at the browser toolbar” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

21. In my opinion, the term “generating, via the browser toolbar” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

22. In my opinion, the term “generating, at a browser toolbar” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

23. In my opinion, the term “determining, at a browser toolbar” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

24. In my opinion, the term “decrypting, at the browser toolbar” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

25. In my opinion, the term “providing, via the browser toolbar, the stored account information to the web service” fails to inform with reasonable certainty a person of ordinary skill in the art in 2008-2009 about the scope of the claimed invention.

## V. THE PATENTS-IN-SUIT AND RELEVANT TECHNOLOGY

### A. Background Technology

26. For the purposes of this case, it is useful to have an understanding of encryption technologies and online ecommerce and web browser technologies.

#### 1. Encryption Technologies

27. Cryptography is a technical field that deals with secret communications. Mathematical algorithms are used to encrypt and decrypt digital data, and keys are used as inputs to algorithms. There are two basic types of cryptographic algorithms using keys: symmetric-key algorithms and public-key algorithms (also referred to asymmetric-key algorithms). See Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C” (2nd ed., 1996), John Wiley & Sons, Inc., USA (“Applied Cryptography”) at 4.

28. In symmetric-key algorithms, the same key is used to encrypt a given message to get a ciphertext and to decrypt the ciphertext to get the given data message. For example, if Device A wants to encrypt data, it can do so using a symmetric algorithm with a symmetric key. If Device B wants to decrypt the encrypted data, it needs to obtain the same symmetric key. This means that Device B must have a way of obtaining the key that does not compromise the key’s secrecy. *Id.* at 4-5.

29. Symmetric-key technologies benefit from rapid computation (such as encryption or decryption,) which is of importance in contexts where large messages are to be encrypted and decrypted. However, a drawback of symmetric-key technologies is that both the sender of an encrypted message and the recipient of the encrypted message need to know the same key (i.e., the symmetric key), and that this key needs to be securely obtained by both the sender and recipient, without any other party learning the key. *Id.*

30. Public-key (asymmetric) algorithms use pairs of keys called public keys and private keys. Each device has a public key that can be accessed by anyone (that is, it is not kept secret) and a corresponding private key that the device keeps secret. *Id.* at 4-5, 31-32.

31. If Device A wants to send data securely to Device B using a public-key algorithm, Device A will encrypt the data using Device B's public key; then Device B will be able to decrypt it using its own corresponding private key. Public-key algorithms were well-known and widely used by 2008. One such algorithm is referred to as RSA, which was developed by R.L. Rivest, A. Shamir, and L. Adleman in 1977 and adopted as a standard in the late 1990s. B. Kaliski, PKCS #1: RSA Encryption Version 1.5, RFC 2313 (Informational) (March 1998), available at <https://datatracker.ietf.org/doc/html/rfc2313>; Microsoft Computer Dictionary (5th ed., 2002) at 459 ("RSA").

32. Asymmetric-key algorithms (i.e., public-key algorithms) enable an elegant bootstrapping of the communicating parties with respect to the keys used to encrypt and decrypt: a first party can generate two related keys, the public key and the private key, and transmit the public key to one or more other parties, who, using this key can encrypt messages for the first party, where no party but the first party can decrypt these. More specifically, if a second party encrypts a message for using a public key distributed by the first party, and a third party intercepts this encrypted message, then the third party cannot decrypt, even if it has also received the public key of the first party.

## **2. Online Ecommerce and Web Browsers**

33. Ecommerce corresponds to the activity of buying or selling products and services over the Internet, and includes activities such as transferring funds, and protecting financial information, user credentials and other sensitive information. Examples of well recognized ecommerce providers include Amazon and eBay.

34. As the specification of the Patents-in-Suit describes, by the time of the invention of the Patents-in-Suit, some customers used “customer account data storage programs” called “digital wallets” to store information used in e-commerce transactions. *See* ’122 Patent at 1:37-43; *see also* Microsoft Computer Dictionary (5th ed., 2002) at 561-62 (“wallet”).

35. To access ecommerce service providers, consumers would use browsers, such as Netscape Navigator (released in 1994), which incorporated SSL encryption to secure transactions, to curb abuse in the context of transmission of sensitive information, including financially sensitive information, transmitted over the Internet.

36. Many users were interested in customizing their browsers, e.g., using browser plugins (sometimes referred to<sup>1</sup> as “extensions.”) A browser plugin is a piece of executable software designed to work with other software. These are components that add a feature (e.g., to a browser), where the feature may block cookies or advertisements, provide security, or add other features of interest to the user. *See* “Internet Explorer Developer Center – Browser Extensions” (Sept. 1, 2008); “Mozilla Developer Center – Extensions” (Sept. 1, 2008); “Mozilla Developer Center – Plugins” (Nov. 13, 2008)); *see also* Microsoft Computer Dictionary (5th ed., 2002) at 409 (“plug-in”). Microsoft Internet Explorer was the first major browser to support plugins/extensions with the release of IE version 4 in 1999. Mozilla Firefox browser started supporting them in 2004.

37. One kind of browser plugin that was common in the early 2000s was a “browser toolbar,” a plug-in that added a user interface toolbar and associated functionality to the browser. *See* “Internet Explorer Developer Center – Internet Explorer Architecture” (May 10, 2008).

---

<sup>1</sup> Extensions commonly comprise source code, whereas plugins always are executables—binary code as opposed to human-readable—their functionality and use overlaps to the extent that the two terms are commonly used interchangeably.

## **VI. CLAIM CONSTRUCTION PRINCIPLES**

38. I understand that claim construction is the process by which a court determines, as a matter of law, the scope and meaning of terms used in the claims of a patent. I further understand that the goal of this process is to give claim terms the ordinary and customary meaning they would have had to a person of ordinary skill in the art at the time of the invention, after reading the entire patent and prosecution history.

39. I understand that the prosecution history of a patent can inform the meaning of some claim language and must be taken into account in construing the claims.

40. I understand that, in some cases, the court may consider extrinsic evidence, such as technical dictionaries, treatises, and expert opinions, to understand the underlying technology and the way in which claim terms would be understood by a POSITA at the relevant time. However, such extrinsic evidence should not be used to vary, contradict, expand, or limit the claim language from how it is defined in the specification or prosecution history.

41. I understand that a patent will be held invalid for indefiniteness if its claims, viewed in light of the specification and prosecution history, fail to inform with reasonable certainty those skilled in the art about the scope of the invention. I further understand that definiteness is to be evaluated from the perspective of someone with skill in the relevant art at the time that the patent was filed.

## **VII. LEVEL OF ORDINARY SKILL IN THE ART**

42. Having reviewed the Patents-in-Suit, in my opinion, a person of ordinary skill in the art would have had a working knowledge of electronic commerce on the World Wide Web and understood security and encryption issues relating to the same. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and one or

more years of professional experience relating to web technologies, security and encryption, or without said professional experience, further education relating to those topics.

43. For the purpose of this declaration, I understand the time of invention to be in the 2008–2009 timeframe.

44. I have applied this definition for purposes of my analysis in this declaration, but I note that my opinions would not change if a slightly higher or lower degree of expertise were applied, because I am analyzing terminology that would be interpreted the same among persons having different skill levels.

## **VIII. OPINIONS REGARDING THE PATENTS-IN-SUIT**

### **A. “securely storing the account information . . .” terms**

45. I understand the parties have proposed the following constructions:

<b>Term</b>	<b>Liberty Peak Construction</b>	<b>Zoho Construction</b>
<b>“securely storing the account information at the browser toolbar”</b> ’122 Claim 1	Plain and ordinary meaning – no need for construction.	Indefinite, or in the alternative: “storing the account information in a data storage implementation wherein the stored account information is accessible only by the browser toolbar”
<b>“securely storing, by the browser toolbar, the account information at the browser toolbar”</b> ’901 Claims 1 and 11 ’088 Claim 1	Plain and ordinary meaning – no need for construction.	Indefinite, or in the alternative: “storing the account information in a data storage implementation wherein the stored account information is accessible only by the browser toolbar”

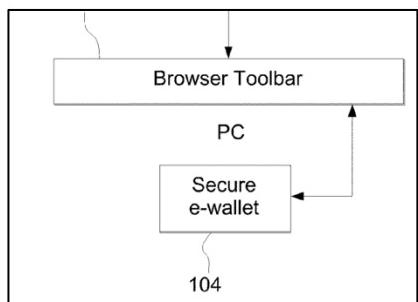
46. The term “securely storing the account information at the browser toolbar” appears in claim 1 of the ’122 Patent. The functionally identical term, “securely storing, by the browser toolbar, the account information at the browser toolbar” appears in claims 1 and 11 of the ’901 Patent and claim 1 of the ’088 Patent.

47. In my opinion, these terms are indefinite because they fail to provide reasonable certainty to a person of ordinary skill in the art as to their meaning because 1) nothing in the written description explains what it means to store account information “at a toolbar” (i.e., software) and, without guidance from specification, a person of ordinary skill in the art would not know what this element means, and 2) “securely storing” is a term of degree—something can be more or less secure and whether information is deemed securely stored is subjectively measured—and because the patent never provides any guidance as to what it means, other than excluding encryption as the means of securely storing, a skilled artisan would not know what it means to store information “securely” as the term is used in the claims. Thus, a POSITA cannot determine what the boundaries of the claim are and cannot reliably determine when infringement occurs.

48. With respect to the first issue—the storage of account information “at a toolbar,” the shared specification of the Patents-in-Suit never describes storing account information at a browser toolbar. Rather, in every instance, the inventors describe storing such data at an e-wallet accessed by the toolbar. *See ’122 patent at 4:14-16 (“a secure e-wallet 104 to securely access and store PII data”); 5:57-61 (“browser toolbar 102 decrypts the PII data and stores it in secure e-wallet ... customer can retrieve the stored PII data from secure e-wallet”); 6:1-3 (“the PII data stored in secure e-wallet 104 is deleted upon the customer closing the current web browser session”); 6:11-12 (“using PII data stored in secure e-wallet”); 6:13-16 (“browser toolbar 102*

can check to see if the PII data currently stored in the secure e-wallet 102 needs to be updated”); 6:19-20 (“the PII data stored in the secure e-wallet 102 is updated”); 6:62-64 (“decrypted PII data is stored in an e-wallet”). This makes sense, since an e-wallet is intended for data storage and is explicitly defined as such in the specification. *See* ’122 patent at 3:62-66 (“An ‘e-wallet’ as used herein refers to any data storage implementation which allows data associated with a customer to be stored and used to make electronic commerce transactions.”).

49. Until late in the prosecution of the ’122 Patent, every independent claim included a limitation requiring that “the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet).” In the final round of claim amendments made in response to rejections under 35 U.S.C. § 101, this limitation was removed, and, in claim 1, replaced with “securely storing the account information at the browser toolbar.” *Compare* ’122 File History, November 11, 2014 Office Action Response at 2-7 *with* ’122 File History, March 2, 2015 Office Action Response at 2-10. As the specification explains, the e-wallet and browser toolbar are distinct from each other. *See* Fig. 1 (left); *id.* at 6:67-7:2 (“FIG. 3



is described with respect to the following entities and functional modules: e-wallet 302, browser toolbar 304,...”); *see also* Fig. 2 (showing e-wallet 210 as separate from the browser toolbar, blocks 207-209). In fact, the applicants explicitly distinguished the toolbar from the e-wallet during prosecution, arguing that: “claim 1 recites ‘using an encryption key maintained by the browser toolbar and inaccessible outside of the browser toolbar.’ This stands in contrast to a digital wallet that might store encrypted data, but leave the key exposed.” ’122 File History, March 2, 2015 Office Action Response at 12.

50. I understand that the parties agree that the browser toolbar is “a software program that adds functionality to a browser and includes a graphical user interface component within the browser.” Like all software, the browser toolbar is made up of executable instructions. It is not a storage location and it would be impossible to store anything “at” it.

51. Thus, the issued claim element requires storing data “at” a toolbar, which is nonsensical to a person of skill in the art. In practice, software may store data in various storage implementations such as in ephemeral memory (RAM), an attached disk or other storage device, or via another piece of software that stores data in one of those locations, such as a database. Data is not stored “at” software and the concept of doing so is nonsensical. To analogize, software is a series of instructions like the words of a recipe. The recipe might itself be stored in a storage location, such as written on a notecard placed in a cupboard, much like software itself is typically stored in binary form on a disk. You can store flour in the same cupboard as the recipe card just like you can store software and data on a disk—storing both the instructions and the ingredients in the same storage location. But you cannot store ingredients (data) inside the words of the recipe (instructions).

52. These limitations are also indefinite because there is no objective definition of what it means to store information “securely.” The specification explains in detail that storing data on a customer computer is insecure, and that mitigating that insecurity is the fundamental problem the invention purports to solve. *See* ’122 patent at 1:23-25 (“Customer account data which is stored, even temporarily, on a customer’s computing device is potentially at risk due to these malicious entities.”); 1:51-54 (“One legitimate concern is that the information that is manually or automatically loaded at the customer’s device can be exposed to rogue programs running on the customer’s computing device.”). 1:59-65 (“Once the customer account data is

received by the customer computing device, however, the data is decrypted for use by the customer (e.g., viewing or storage) and may then be intercepted, snooped, or otherwise accessed by rogue programs running on the customer's device.”). But the specification never explains what it means to “securely store.”

53. From the perspective of a person of skill in the art at the time of the Patents-in-Suit, whether a computer system or means of storing information is “secure” is not a yes-or-no proposition; it is a matter of degree. This is similar to security in everyday applications. For example, consider a house. A house with a closed door is more secure than a house with an open door, and one with a locked door is more secure than either. Houses with alarms or guard dogs are more secure than those without, and one with an armed guard at each entrance is even more so. Which of these security measures makes the house “secure” depends on the needs of the house’s occupants and what threats they want to protect the house from.

54. Like houses, there are various measures known to a person of skill in the art that could be taken to secure data on a computer system. For example, requiring user passwords is more secure than leaving a computer system unlocked at all times. Randomizing memory locations can make it harder to retrieve sensitive information from an otherwise known address. To be more secure, certain hardware storage can be made cryptographically secure and only openable with user interaction, such as a fingerprint or separate password input directly into the hardware device. Systems can try to prevent “rogue programs” like those described by the specification from running by preventing software that is not cryptographically verified from running on the computer.

55. While many techniques known in the art can make stored information more secure than not using them, there is no clear boundary delineating securely stored information

from insecurely stored information, as that term is used in the patents. The Patents-in-Suit do not explain what is or is not secure; neither the written description nor the prosecution history provide any guidance in answering these questions. The specification merely states data is stored in a “secure” e-wallet. *E.g.* ’122 patent at 5:57-59 (“After receipt of the encrypted PII data, browser toolbar 102 decrypts the PII data and stores it in secure e-wallet 104.”). And while the specification does describe what an “e-wallet” is, it says nothing about what a “secure” e-wallet is or how it functions.

56. While the specification does discuss encryption as a way to secure data, it teaches that the e-wallet, and thus the “storage” is secure in some other way. In every embodiment the data is first decrypted and then stored in an e-wallet. *See* ’122 patent at 5:53-61 (“After receipt of the encrypted PII data, browser toolbar 102 decrypts the PII data and stores it in secure e-wallet 104.”); 6:58-64 (“Encrypted PII data is then transmitted to the browser toolbar at the customer’s computer system, block 208, for decryption, block 209, by the browser toolbar. The decrypted PII data is stored in an e-wallet, block 210, for use by the customer.”). Further, the Background of the Invention describes “one technical challenge” as allowing “sensitive customer account data, to be **transmitted to a computing device and decrypted** within the receiving computing device such that the data is not exposed to malicious entities external or internal to the computing device.” ’122 Patent at 2:5-9 (emphasis added). The applicants also emphasized this functionality during prosecution to overcome rejections over the prior art:

Applicants discussed with the Examiner the purpose of the system, which is to safeguard a user’s data from theft/attack after the data is downloaded and decrypted by the user’s computer, and before the user is permitted access to the data. To this end, Applicants clarified that **the system saves the decrypted data to a secure e-wallet** prior to giving a user access to the data, thereby preventing the data from being accessed by rogue programs running on the user’s device (as per paragraph [0007] of the originally-filed specification).

'122 File History, March 21, 2011 Office Action Response at 8; *id.* at 9 (“Further, on receipt of encrypted data, the browser toolbar may decrypt and save the data to a secure e-wallet prior to giving a user access to the data, thereby preventing attacks on the data by rogue programs running on the user’s system.”). And the Examiner cited this as one of the reasons for allowing the pre-101 rejection claims. *See* '122 File History, April 30, 2014 Notice of Allowance at 8-9 (“[O]n receipt of encrypted data, the browser toolbar may decrypt and save the data to a secure e-wallet prior to giving a user access to the data, thereby preventing attacks on the data by rogue programs running on the user’s system.”).

57. Given the lack of any guidance about what the inventors considered to be “secure,” and the explicit instructions that is not encryption—the only form of security otherwise discussed in the written description—there is no way for a person of ordinary skill in the art to know what is and is not encompassed by the claims. All a person of skill in the art is instructed to do is to put decrypted data in a “secure e-wallet,” but the claims are not directed to storing in an e-wallet.

58. Thus, in my opinion, the “securely storing” limitations are indefinite because they fail to provide reasonable certainty to a person of ordinary skill in the art as to their meaning.

#### **B. Steps Performed “via the browser toolbar” and “at the browser toolbar”**

59. I understand the parties have proposed the following constructions:

Term	Liberty Peak Construction	Zoho Construction
“generating, via the browser toolbar” '122 Claim 7	Plain and ordinary meaning – no need for construction.	Indefinite

<b>Term</b>	<b>Liberty Peak Construction</b>	<b>Zoho Construction</b>
<b>“generating, at a browser toolbar”</b> ’901 Claims 1 and 11 ’088 Claim 1	Plain and ordinary meaning – no need for construction.	Indefinite
<b>“determining, at a browser toolbar”</b> ’122 Claim 15 ’088 Claim 15	Plain and ordinary meaning – no need for construction.	Indefinite
<b>“decrypting, at the browser toolbar”</b> ’122 Claim 15	Plain and ordinary meaning – no need for construction.	Indefinite
<b>“providing, via the browser toolbar, the stored account information to the web service”</b> ’122 Claim 6	Plain and ordinary meaning – no need for construction.	Indefinite

60. I understand that the doctrine of claim differentiation means that there is presumed to be a difference in meaning and scope when different words or phrases are used in separate claims. In my opinion, these terms are indefinite because they fail to provide reasonable certainty to a person of ordinary skill in the art as to their meaning because there is nothing to explain what it means for an action to be performed “via” or “at” software (the browser toolbar), rather than “by” the browser toolbar, as recited elsewhere in the claims.

61. To illustrate, the meaning of “decrypting by the browser toolbar” in claim 1 of the ’122 patent is straightforward: the software that is the browser toolbar executes a decryption process. “Decrypting, **at** the browser toolbar,” recited in claim 15 of the ’122 patent, has a presumptively different meaning, but what it is remains ambiguous.

62. The same issue obtains for the rest of the terms above—they mean different things, but there is no guidance as to what those meanings are. That is, I understand that “generating [a key], via the browser toolbar” is presumed to have a different meaning than “generating [a key], at a browser toolbar,” but what each would mean if different is wholly unclear to a person of ordinary skill in the art.

63. For these reasons, it is my opinion that the above limitations are indefinite.

## **IX. SUPPLEMENTATION**

64. I reserve the right to supplement this report based on additional information, including to respond to any different or additional constructions proposed by LPV or any additional identification of alleged support for the means-plus-function terms I discuss above. In particular, I have not yet seen what intrinsic or extrinsic evidence LPV may rely on to support its positions, and LPV has yet to propose constructions for certain of the disputed terms.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code. This declaration was executed on January 6, 2023 in Tokyo Japan.



---

Markus Jakobsson

# Appendix A

# CV and Research Statement

Markus Jakobsson  
[www.linkedin.com/in/markusjakobsson](https://www.linkedin.com/in/markusjakobsson)  
[www.markus-jakobsson.com](http://www.markus-jakobsson.com)

## 1 At a Glance

- **Focus.** *Identification of security problems, trends and solution along four axes – computational, structural, physical and social; quantitative and qualitative fraud analysis; development of disruptive security technologies.*
- **Education.** *PhD* (Computer Science/Cryptography, University of California at San Diego, 1997); *MSc* (Computer Science, University of California at San Diego, 1994); *MSc* (Computer Engineering, Lund Institute of Technology, Sweden, 1993).
- **Large research labs.** *San Diego Supercomputer Center* (Researcher, 1996-1997); *Bell Labs* (Member of Technical Staff, 1997-2001); *RSA Labs* (Principal Research Scientist, 2001-2004); *Xerox PARC* (Principal Scientist, 2008-2010); *PayPal* (Principal Scientist of Consumer Security, Director, 2010-2013); *Qualcomm* (Senior Director, 2013-2015); *Agari* (Chief Scientist, 2016–2018); *Amber Solutions Inc* (Chief of Security and Data Analytics, 2018 – 2019); *ByteDance* (Principal Scientist, 2020-2021)
- **Academia.** *New York University* (Adjunct Associate Professor, 2002-2004); *Indiana University* (Associate Professor & Associate Director, 2004-2008; Adjunct Associate Professor, 2008-2016).
- **Entrepreneurial activity.** *ZapFraud* (Anti-scam technology; CTO and founder, 2012-current); *RavenWhite Security* (Authentication solutions; CTO and founder, 2005-); *RightQuestion* (Consulting; Founder, 2007-current); *FatSkunk* (Malware detection; CTO and founder, 2009-2013 – FatSkunk was acquired by Qualcomm); *LifeLock* (Id theft protection; Member of fraud advisory board, 2009-2013); *CellFony* (Mobile security; Member of technical advisory board, 2009-2013); *PopGiro* (User Reputation; Member of technical advisory board, 2012-2013); *MobiSocial* (Social networking, Member of technical advisory board, 2013); *Cequence Security* (Anti-fraud, Member of technical advisory board, 2013–current)
- **Anti-fraud consulting.** *KommuneData* [Danish govt. entity] (1996); *J.P. Morgan Chase* (2006-2007); *PayPal* (2007-2011); *Boku* (2009-2010); *Western Union* (2009-2010).

- **Intellectual Property, Testifying Expert Witness.** *Inventor of 100+ patents; expert witness in 25+ patent litigation cases* (McDermott, Will & Emery; Bereskin & Parr; WilmerHale; Hunton & Williams; Quinn Emanuel Urquhart & Sullivan; Freed & Weiss; Berry & Domer; Fish & Richardson; DLA Piper; Cipher Law Group; Keker & Van Nest). Details and references upon request.
- **Publications.** Books: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crime-ware: Understanding New Attacks and Defenses* (Symantec Press, 2008); *Towards Trustworthy Elections: New Directions in Electronic Voting* (Springer Verlag, 2010); *Mobile Authentication: Problems and Solutions* (Springer Verlag, 2012); *The Death of the Internet* (Wiley, 2012); *Understanding Social Engineering* (Springer Verlag, 2016); *Security, Privacy and User Interaction* (Springer Verlag, 2020); 100+ peer-reviewed publications

## 2 At a Glance

Ten years before Bitcoin was created, I formalized the notion of Proof of Work and described its use for mining of crypto payments. I later developed energy-efficient alternatives to this paradigm, and showed how to enable mining on mobile devices, which is not possible for Bitcoin. I am the founder of the academic discipline of phishing and have developed techniques to predict fraud trends years before they emerge, enabling countermeasures to be developed before they are needed. I developed the notion of implicit authentication, which is now ubiquitous; I also founded a company that developed the first retroactive virus detection technology, with guarantees of detection; the company was acquired by Qualcomm in 2013. I have worked as chief scientist and similar positions in startups as well as industry behemoths, such as PayPal. I have several hundred patents to my name and am a prominent security researcher with hundreds of peer reviewed publications and an array of textbooks. My 1997 PhD thesis, from University of California at San Diego, was on distributed electronic payment systems with revocable privacy.

## 3 Work History (Highlights)

1. **Member of Technical Staff, Bell Labs (1997-2001).** Markus was part of the security research group at Bell Labs. He formalized the notion of *proof of work*, later an integral part of BitCoin.
2. **Principal Scientist, RSA Labs (2001-2005).** Markus posited that phishing would become a mainstream problem, and developed ethical techniques for identifying likely trends based on human subject experiments.
3. **Associate Professor, Indiana University (2005-2008).** Markus was hired to lead the newly formed security group at Indiana University, and

created a research group comprising approximately 10 professors and 30 students, studying social engineering and fraud.

4. **Principal Scientist, Xerox PARC (2008-2010).** Markus was hired to lead the research efforts of the Xerox PARC security group, and developed the notion of *implicit authentication*, a technology that is now ubiquitous.
5. **Principal Scientist, PayPal (2010-2013).** Markus did research on security and user interfaces, and developed techniques to reduce the losses associated with *liar buyer fraud*.
6. **Senior Director, Qualcomm (2013-2016).** Qualcomm acquires FatSkunk, a company founded by Markus. At FatSkunk, Markus developed *retroactive* malware detection with provable security guarantees. A simplified version of this is now deployed with almost all Qualcomm chipsets.
7. **Chief Scientist, Agari (2016-2018).** Markus developed a technique to acquire fraudster intelligence by compromising scammer email accounts – *while staying within the law* – resulting in the extradition of several African scam lords to the U.S.
8. **Chief of Security and Data Analytics, Amber Solutions (2018-2020).** Markus developed usable configuration methods supporting improved security and privacy for IoT installations.
9. **Chief Scientist, ByteDance (2020-2021).** Markus oversaw the establishment of a research group and a research agenda at ByteDance, and contributed to their intellectual property and product security.
10. **Chief Scientist, Artema LABS (2021-).** Managing the research, product strategy, and patent strategy for Artema LABS, a Los Angeles based startup in the Crypto/NFT sector.

## 4 Publication List

Books (1-8); book chapters, journals, conference publications and other scientific publications (9-147), issued /published U.S. patents (148-234). For an updated list, and for international patents, please see [www.markus-jakobsson.com/publications](http://www.markus-jakobsson.com/publications) and appropriate patent search engines.

## References

- [1] M. Jakobsson, *Security, Privacy and User Interaction*, ISBN 978-3-030-43753-4, 110 pages, 2020.
- [2] M. Jakobsson, *Understanding Social Engineering Based Scams*, ISBN 978-1-4939-6457-4, 130 pages, Springer, 2016.

- [3] M. Jakobsson, *Mobile Authentication: Problems and Solutions*, ISBN 1461448778, 125 pages, Springer, 2013.
- [4] M. Jakobsson, (editor) *The Death of the Internet*, ASIN B009CN2JVE, 359 pages, IEEE Computer Society Press, 2012.
- [5] D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. Ryan, J. Benaloh, and M. Kutylowski, (editors), *Towards Trustworthy Elections: New Directions in Electronic Voting*, 411 pages, (Vol. 6000), Springer, 2010.
- [6] M. Jakobsson and Z. Ramzan (editors), *Crimeware: Trends in Attacks and Countermeasures*, ISBN 0321501950, Hardcover, 582 pages, Symantec Press / Addison Wesley, 2008.
- [7] M. Jakobsson and S. A. Myers (editors), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, ISBN 0-471-78245-9, Hardcover, 739 pages, Wiley, 2006.
- [8] M. Jakobsson, M. Yung, J. Zhou, *Applied Cryptography and Network Security: Second International Conference , Yellow Mountain, China, 2004*, 511 pages, Lecture Notes in Computer Science (Book 3089), 2004.
- [9] M. Jakobsson, “Permissions and Privacy,” in IEEE Security & Privacy, vol. 18, no. 2, pp. 46-55, March-April 2020
- [10] M. Jakobsson, “The Rising Threat of Launchpad Attacks,” in IEEE Security & Privacy, vol. 17, no. 5, pp. 68-72, Sept.-Oct. 2019
- [11] J Koven, C Felix, H Siadati, M Jakobsson, E Bertini, “Lessons learned developing a visual analytics solution for investigative analysis of scamming activities,” IEEE transactions on visualization and computer graphics 25 (1), 225-234
- [12] M Jakobsson, “Two-factor inauthentication?the rise in SMS phishing attacks” Computer Fraud & Security 2018 (6), 6-8
- [13] M. Dhiman, M. Jakobsson, T.-F. Yen, “Breaking and fixing content-based filtering,” 2017 APWG Symposium on Electronic Crime Research (eCrime), 52-56
- [14] M. Jakobsson, “Addressing sophisticated email attacks,” 2017 International Conference on Financial Cryptography and Data Security, 310-317
- [15] M. Jakobsson, “User trust assessment: a new approach to combat deception,” Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 2016, pages 73-78
- [16] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, “Mind your SMSes: Mitigating social engineering in second factor authentication,” Computers and Security, 2016

- [17] M. Jakobsson, W. Leddy, “Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters,” IEEE Spectrum 53 (5), 2016, 40-55
- [18] N. Sae-Bae, M. Jakobsson, *Hand Authentication on Multi-Touch Tablets*, HotMobile 2014
- [19] Y. Park, J. Jones, D. McCoy, E. Shi, M. Jakobsson, *Scambaiter: Understanding Targeted Nigerian Scams on Craigslist*, NDSS 2014
- [20] D. Balfanz, R. Chow, O. Eisen, M. Jakobsson, S. Kirsch, S. Matsumoto, J. Molina, and P. van Oorschot, “The future of authentication,” Security & Privacy, IEEE, 10(1), 22-27, 2012.
- [21] M. Jakobsson, and H. Siadati, *Improved Visual Preference Authentication: Socio-Technical Aspects in Security and Trust*, (STAST), 2012 Workshop on IEEE, 27–34, 2012.
- [22] M. Jakobsson, R. I. Chow, and J. Molina, “Authentication-Are We Doing Well Enough?[Guest Editors’ Introduction]” Security & Privacy, IEEE, 10(1), 19-21, 2012.
- [23] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, “Implicit authentication through learning user behavior,” Information Security, 99-113, Springer Berlin Heidelberg, 2011.
- [24] M. Jakobsson and K. Johansson, “Practical and Secure Software-Based Attestation,” Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 1–9, 2011.
- [25] A. Juels, D. Catalano, and M.Jakobsson, *Coercion-resistant electronic elections: Towards Trustworthy Elections*, 37–63, Springer Berlin Heidelberg, 2010.
- [26] M. Jakobsson and F. Menczer, “Web Forms and Untraceable DDoS Attacks,” in Network Security, Huang, S., MacCallum, D., and Du, D. Z., Eds.,77–95, Springer, 2010.
- [27] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, “Authentication in the Clouds: A Framework and its Application to Mobile Users,” 2010.
- [28] X. Wang, P. Golle, M. Jakobsson, and A. Tsow, “Deterring voluntary trace disclosure in re-encryption mix-networks,” ACM Trans. Inf. Syst. Secur., 13(2), 1-24, 2010.
- [29] X. Wang, P. Golle, M. Jakobsson, A.Tsow, “Deterring voluntary trace disclosure in re-encryption mix-networks,” ACM Trans. Inf. Syst. Secur. 13(2): (2010)

- [30] M. Jakobsson, and C. Soghoian, “Social Engineering in Phishing,” Information Assurance, Security and Privacy Services, 4, 2009.
- [31] M. Jakobsson, C. Soghoian and S. Stamm, “Phishing,” Handbook of Financial Cryptography (CRC press, 2008)
- [32] M. Jakobsson and A. Tsow, “Identity Theft,” In John R. Vacca, Editor, “Computer And Information Security Handbook” (Morgan Kaufmann, 2008)
- [33] S. Srikanth and M. Jakobsson, “Using Cartoons to Teach Internet Security,” Cryptologia, vol. 32, no. 2, 2008
- [34] M. Jakobsson, N. Johnson and P. Finn, “Why and How to Perform Fraud Experiments,” IEEE Security and Privacy, March/April 2008 (Vol. 6, No. 2) pp. 66-68
- [35] M. Jakobsson and S. Myers, “Delayed Password Disclosure,” International Journal of Applied Cryptography, 2008, pp. 47-59.
- [36] M. Jakobsson and S. Stamm, “Web Camouflage: Protecting Your Clients from Browser Sniffing Attacks,” IEEE Security & Privacy Magazine. November/December 2007
- [37] P. Finn and M. Jakobsson, “Designing and Conducting Phishing Experiments,” IEEE Technology and Society Magazine, Special Issue on Usability and Security
- [38] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer. “Social Phishing,” The Communications of the ACM, October 2007
- [39] A. Tsow, M. Jakobsson, L. Yang and S. Wetzel, “Warkitting: the Drive-by Subversion of Wireless Home Routers,” Anti-Phishing and Online Fraud, Part II Journal of Digital Forensic Practice, Volume 1, Special Issue 3, November 2006
- [40] M. Gandhi, M. Jakobsson and J. Ratkiewicz, “Badvertisements: Stealthy Click-Fraud with Unwitting Accessories,” Anti-Phishing and Online Fraud, Part I Journal of Digital Forensic Practice, Volume 1, Special Issue 2, November 2006
- [41] N. Ben Salem, J.-P. Hubaux and M. Jakobsson. “Reputation-based Wi-Fi Deployment,” Mobile Computing and Communications Review, Volume 9, Number 3 (Best papers of WMASH 2004)
- [42] N. Ben Salem, J. P. Hubaux, and M. Jakobsson. “Node Cooperation in Hybrid Ad hoc Networks,” IEEE Transactions on Mobile Computing, Vol. 5, No. 4, April 2006.
- [43] P. MacKenzie, T. Shrimpton, and M. Jakobsson. “Threshold Password-Authenticated Key Exchange,” Journal of Cryptology, 2005

- [44] A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. “How To Turn Loaded Dice Into Fair Coins.” IEEE Transactions on Information Theory, vol. 46(3). May 2000. pp. 911–921.
- [45] M. Jakobsson, P. MacKenzie, and J.P. Stern. “Secure and Lightweight Advertising on the Web,” Journal of Computer Networks, vol. 31, issue 11–16, Elsevier North-Holland, Inc., 1999. pp. 1101–1109.
- [46] M. Jakobsson, “Cryptographic Protocols,” Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.
- [47] M. Jakobsson, “Cryptographic Privacy Protection Techniques,” Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.
- [48] M. Jakobsson, E. Shi, P. Golle, R. Chow, “Implicit authentication for mobile devices,” 4th USENIX Workshop on Hot Topics in Security (HotSec ’09); 2009 August 11; Montreal, Canada.
- [49] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, “Controlling data in the cloud: outsourcing computation without outsourcing control,” Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009); 2009 November 13; Chicago, IL. NY: ACM; 2009; pp. 85–90.
- [50] M. Jakobsson, H. Siadati, M. Dhiman, “Liar Buyer Fraud, and How to Curb It,” NDSS, 2015
- [51] M. Jakobsson, T.-F. Yen, “How Vulnerable Are We To Scams?,” BlackHat, 2015
- [52] M. Jakobsson, “How to Wear Your Password,” BlackHat, 2014
- [53] M. Jakobsson and G. Stewart, “Mobile Malware: Why the Traditional AV Paradigm is Doomed, and How to Use Physics to Detect Undesirable Routines,” in BlackHat, 2013.
- [54] M. Jakobsson, and H. Siadati, “SpoofKiller: You Can Teach People How to Pay, but Not How to Pay Attention” in Socio-Technical Aspects in Security and Trust (STAST), 2012 Workshop on, 3-10, 2012.
- [55] M. Jakobsson, and M. Dhiman, “The benefits of understanding passwords,” in Proceedings of the 7th USENIX conference on Hot Topics in Security, Berkeley, CA, USA, 2012.
- [56] M. Jakobsson, and S. Taveau, “The Case for Replacing Passwords with Biometrics,” Mobile Security Technologies, 2012.
- [57] M. Jakobsson and D. Liu, “Bootstrapping mobile PINs using passwords,” W2SP, 2011.

- [58] M. Jakobsson and R. Akavipat, “Rethinking passwords to adapt to constrained keyboards,” 2011.
- [59] Y. Niu, E. Shi, R. Chow, P. Golle, and M. Jakobsson, “One Experience Collecting Sensitive Mobile Data,” In USER Workshop of SOUPS, 2010.
- [60] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, “Implicit Authentication through Learning User Behavior,” 2010.
- [61] M. Jakobsson and K. Johansson, Assured Detection of Malware With Applications to Mobile Platforms, 2010.
- [62] M. Jakobsson and K. Johansson, “Retroactive Detection of Malware With Applications to Mobile Platforms,” in HotSec 2010, Washington, DC, 2010.
- [63] M. Jakobsson, A Central Nervous System for Automatically Detecting Malware, 2009.
- [64] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, J. Molina, E. Shi, and J. Staddon, “Controlling data in the cloud: outsourcing computation without outsourcing control,” ACM workshop on Cloud computing security (CCSW), 2009.
- [65] M. Jakobsson and A. Juels, “Server-Side Detection of Malware Infection,” in New Security Paradigms Workshop (NSPW), Oxford, UK, 2009.
- [66] M. Jakobsson, “Captcha-free throttling,” Proceedings of the 2nd ACM workshop on Security and artificial intelligence, 15–22, 2009.
- [67] M. Jakobsson, E. Shi, P. Golle, and R. Chow, “Implicit authentication for mobile devices,” Proceedings of the 4th USENIX conference on Hot topics in security, 9–9, 2009.
- [68] C. Soghoian, O. Friedrichs and M. Jakobsson, “The Threat of Political Phishing,” International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)
- [69] R. Chow, P. Golle, M. Jakobsson, L. Wang and X. Wang, “Making CAPTCHAs Clickable,” In proc. of HotMobile 2008.
- [70] M. Jakobsson, A. Juels, and J. Ratkiewicz, “Privacy-Preserving History Mining for Web Browsers,” Web 2.0 Security and Privacy, 2008.
- [71] M. Jakobsson, E. Stolterman, S. Wetzel, L. Yang, “Love and Authentication,” (Notes) ACM Computer/Human Interaction Conference (CHI), 2008. Also see [www.I-forgot-my-password.com](http://www.I-forgot-my-password.com)
- [72] M. Jakobsson and S. Myers, “Delayed Password Disclosure,” Proceedings of the 2007 ACM workshop on Digital Identity Management
- [73] M. Jakobsson, S. Stamm, Z. Ramzan, “JavaScript Breaks Free,” W2SP ’07

- [74] A. Juels, S. Stamm, M. Jakobsson, “Combatting Click Fraud via Premium Clicks,” USENIX Security 2007
- [75] R. Chow, P. Golle, M. Jakobsson, X. Wang, “Clickable CAPTCHAs,” Ad-Fraud ’07 Workshop; 2007 September 14; Stanford, CA, USA
- [76] S. Stamm, Z. Ramzan, and M. Jakobsson, “Drive-by Pharming,” In Proceedings of Information and Communications Security, 9th International Conference, ICICS 2007
- [77] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, “What Instills Trust? A Qualitative Study of Phishing,” USEC ’07.
- [78] R. Akavipat, V. Anandpara, A. Dingman, C. Liu, D. Liu, K. Pongsanon, H. Roinestad and M. Jakobsson, “Phishing IQ Tests Measure Fear, not Ability,” USEC ’07.
- [79] M. Jakobsson, “The Human Factor in Phishing,” American Conference Institute’s Forum on Privacy & Security of Consumer Information, 2007
- [80] S. Srikwan, M. Jakobsson, A. Albrecht and M. Dalkilic, “Trust Establishment in Data Sharing: An Incentive Model for Biodiversity Information Systems,” TrustCol 2006
- [81] J.Y. Choi, P. Golle, M. Jakobsson, “Tamper-Evident Digital Signatures: Protecting Certification Authorities Against Malware,” DACS ’06
- [82] L. Yang, M. Jakobsson, S. Wetzel, “Discount Anonymous On Demand Routing for Mobile Ad hoc Networks,” SECURECOMM ’06
- [83] P. Golle, X. Wang, M. Jakobsson, A. Tsow, “Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks.” IEEE S&P ’06
- [84] M. Jakobsson, A. Juels, T. Jagatic, “Cache Cookies for Browser Authentication (Extended Abstract),” IEEE S&P ’06
- [85] M. Jakobsson and J. Ratkiewicz, “Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features.”, WWW ’06
- [86] M. Jakobsson and S. Stamm. “Invasive Browser Sniffing and Countermeasures,” WWW ’06
- [87] J.Y. Choi, P. Golle and M. Jakobsson. “Auditable Privacy: On Tamper-Evident Mix Networks,” Financial Crypto ’06
- [88] A. Juels, D. Catalano and M. Jakobsson. “Coercion-Resistant Electronic Elections,” WPES ’05
- [89] V. Griffith and M. Jakobsson. “Messin’ with Texas, Deriving Mother’s Maiden Names Using Public Records,” ACNS ’05, 2005.

- [90] M. Jakobsson and L. Yang. “Quantifying Security in Hybrid Cellular Networks,” ACNS ’05, 2005
- [91] Y.-C. Hu, M. Jakobsson, and A. Perrig. “Efficient Constructions for One-way Hash Chains,” ACNS ’05, 2005
- [92] M. Jakobsson. “Modeling and Preventing Phishing Attacks,” Phishing Panel in Financial Cryptography ’05. 2005, abstract in proceedings.
- [93] N. Ben Salem, J.-P. Hubaux, and M. Jakobsson. “Reputation-based Wi-Fi Deployment Protocols and Security Analysis,” In WMASH ’04. ACM Press, 2004. pp. 29–40.
- [94] M. Jakobsson and S. Wetzel. “Efficient Attribute Authentication with Applications to Ad Hoc Networks,” In VANET ’04. ACM Press, 2004. pp. 38–46.
- [95] M. Jakobsson, X. Wang, and S. Wetzel. “Stealth Attacks in Vehicular Technologies,” Invited paper. In Proceedings of IEEE Vehicular Technology Conference 2004 Fall (VTC-Fall 2004). IEEE, 2004.
- [96] A. Ambainis, H. Lipmaa, and M. Jakobsson. “Cryptographic Randomized Response Technique,” In PKC ’04. LNCS 2947. Springer-Verlag, 2004. pp. 425–438.
- [97] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. “Universal Re-encryption for Mixnets,” In CT-RSA ’04. LNCS 2964. Springer-Verlag, 2004. pp. 163–178.
- [98] P. Golle and M. Jakobsson. “Reusable Anonymous Return Channels,” In WPES ’03. ACM Press, 2003. pp. 94–100.
- [99] M. Jakobsson, S. Wetzel, B. Yener. “Stealth Attacks on Ad-Hoc Wireless Networks,” In IEEE VTC ’03, 2003.
- [100] N. Ben Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson. “A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks,” In ACM MobiHoc ’03. ACM Press, 2003. pp. 13–24.
- [101] M. Jakobsson, J.-P. Hubaux and L. Buttyan. “A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks,” In FC ’03. LNCS 2742. Springer-Verlag, 2003. pp. 15–33.
- [102] M. Jakobsson, T. Leighton, S. Micali and M. Szydlo. “Fractal Merkle Tree Representation and Traversal,” In RSA-CT ’03 2003.
- [103] A. Boldyreva and M Jakobsson. “Theft protected proprietary certificates,” In DRM ’02. LNCS 2696, 2002. pp. 208–220.

- [104] P. Golle, S. Zhong, M. Jakobsson, A. Juels, and D. Boneh. “Optimistic Mixing for Exit-Polls,” In *Asiacrypt ’02*. LNCS 2501. Springer-Verlag, 2002. pp. 451–465.
- [105] P. MacKenzie, T. Shrimpton, and M. Jakobsson. “Threshold Password-Authenticated Key Exchange,” In *CRYPTO ’02*. LNCS 2442. Springer-Verlag, 2002. pp. 385–400.
- [106] M. Jakobsson. “Fractal Hash Sequence Representation and Traversal,” In *Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT ’02)*. 2002. pp. 437–444.
- [107] M. Jakobsson, A. Juels, and R. Rivest. “Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking,” In *Proceedings of the 11th USENIX Security Symposium*. USENIX Association, 2002. pp. 339–353.
- [108] D. Coppersmith and M. Jakobsson. “Almost Optimal Hash Sequence Traversal,” In *Financial Crypto ’02*. 2002.
- [109] M. Jakobsson. “Financial Instruments in Recommendation Mechanisms,” In *Financial Crypto ’02*. 2002.
- [110] J. Garay, and M. Jakobsson. “Timed Release of Standard Digital Signatures,” In *Financial Crypto ’02*. 2002.
- [111] F. Menczer, N. Street, N. Vishwakarma, A. Monge, and M. Jakobsson. “Intellishopper: A Proactive, Personal, Private Shopping Assistant,” In *AAMAS ’02*. ACM Press, 2002. pp. 1001–1008.
- [112] M. Jakobsson, A. Juels, and P. Nguyen. “Proprietary Certificates,” In *CT-RSA ’02*. LNCS 2271. Springer-Verlag, 2002. pp. 164–181.
- [113] M. Jakobsson and A. Juels. “An Optimally Robust Hybrid Mix Network,” In *PODC ’01*. ACM Press. 2001. pp. 284–292.
- [114] M. Jakobsson and M. Reiter. “Discouraging Software Piracy Using Software Aging,” In *DRM ’01*. LNCS 2320. Springer-Verlag, 2002. pp. 1–12.
- [115] M. Jakobsson and S. Wetzel. “Security Weaknesses in Bluetooth,” In *CT-RSA ’01*. LNCS 2020. Springer-Verlag, 2001. pp. 176–191.
- [116] M. Jakobsson and D. Pointcheval. “Mutual Authentication for Low-Power Mobile Devices,” In *Financial Crypto ’01*. LNCS 2339. Springer-Verlag, 2001. pp. 178–195.
- [117] M. Jakobsson, D. Pointcheval, and A. Young. “Secure Mobile Gambling,” In *CT-RSA ’01*. LNCS 2020. Springer-Verlag, 2001. pp. 110–125.
- [118] M. Jakobsson and S. Wetzel. “Secure Server-Aided Signature Generation,” In *PKC ’01*. LNCS 1992. Springer-Verlag, 2001. pp. 383–401.

- [119] M. Jakobsson and A. Juels. “Addition of ElGamal Plaintexts,” In T. Okamoto, ed., ASIACRYPT ’00. LNCS 1976. Springer-Verlag, 2000. pp. 346–358.
- [120] M. Jakobsson, and A. Juels. “Mix and Match: Secure Function Evaluation via Ciphertexts,” In ASIACRYPT ’00. LNCS 1976. Springer-Verlag, 2000. pp. 162–177.
- [121] R. Arlein, B. Jai, M. Jakobsson, F. Monroe, and M. Reiter. “Privacy-Preserving Global Customization,” In ACM E-Commerce ’00. ACM Press, 2000. pp. 176–184.
- [122] C.-P. Schnorr and M. Jakobsson. “Security of Signed ElGamal Encryption,” In ASIACRYPT ’00. LNCS 1976. Springer-Verlag, 2000. pp. 73–89.
- [123] P. Bohannon, M. Jakobsson, and S. Srikanth. “Cryptographic Approaches to Privacy in Forensic DNA Databases,” In Public Key Cryptography ’00. LNCS 1751. Springer-Verlag, 2000, pp. 373–390.
- [124] J. Garay, M. Jakobsson, and P. MacKenzie. “Abuse-free Optimistic Contract Signing,” In CRYPTO ’99. LNCS 1666. Springer-Verlag, 1999. pp. 449–466.
- [125] M. Jakobsson. “Flash Mixing,” In PODC ’99. ACM Press, 1999. pp. 83–89.
- [126] G. Di Crescenzo, N. Ferguson, R. Impagliazzo, and M. Jakobsson. “How To Forget a Secret,” In STACS ’99. LNCS 1563. Springer-Verlag, 1999. pp. 500–509.
- [127] M. Jakobsson, D. M’Raihi, Y. Tsiounis, and M. Yung. “Electronic Payments: Where Do We Go from Here?,” In CQRE (Secure) ’99. LNCS 1740. Springer-Verlag, 1999. pp. 43–63.
- [128] C.P. Schnorr and M. Jakobsson. “Security Of Discrete Log Cryptosystems in the Random Oracle + Generic Model,” In Conference on The Mathematics of Public-Key Cryptography. 1999.
- [129] M. Jakobsson and A. Juels “Proofs of Work and Breadpudding Protocols,” In CMS ’99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 252 – 272.
- [130] M. Jakobsson and C-P Schnorr. “Efficient Oblivious Proofs of Correct Exponentiation,” In CMS ’99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 71–86.
- [131] M. Jakobsson, P. MacKenzie, and J.P. Stern. “Secure and Lightweight Advertising on the Web,” In World Wide Web ’99

- [132] M. Jakobsson, J.P. Stern, and M. Yung. “Scramble All, Encrypt Small,” In *Fast Software Encryption ’99*. LNCS 1636. Springer-Verlag, 1999. pp. 95–111.
- [133] M. Jakobsson and J. Mueller. “Improved Magic Ink Signatures Using Hints,” In *Financial Cryptography ’99*. LNCS 1648. Springer-Verlag, 1999. pp. 253–268.
- [134] M. Jakobsson. “Mini-Cash: A Minimalistic Approach to E-Commerce,” In *Public Key Cryptography ’99*. LNCS 1560. Springer-Verlag, 1999. pp. 122–135.
- [135] M. Jakobsson. “On Quorum Controlled Asymmetric Proxy Re-encryption,” In *Public Key Cryptography ’99*. LNCS 1560. Springer-Verlag, 1999. pp. 112–121.
- [136] M. Jakobsson and A. Juels. “X-Cash: Executable Digital Cash,” In *Financial Cryptography ’98*. LNCS 1465. Springer-Verlag, 1998. pp. 16–27.
- [137] M. Jakobsson and D. M’Raihi. “Mix-based Electronic Payments,” In *Proceedings of the Selected Areas in Cryptography*. LNCS 1556. Springer-Verlag, 1998. pp. 157–173.
- [138] M. Jakobsson, E. Shriver, B. Hillyer, and A. Juels. “A Practical Secure Physical Random Bit Generator,” In *CCS ’98: Proceedings of the 5th ACM conference on Computer and communications security*. ACM Press, 1998. pp. 103–111.
- [139] M. Jakobsson. “A Practical Mix,” In *Advances in Cryptology – EuroCrypt ’98*. LNCS 1403. Springer-Verlag, 1998. pp. 448–461.
- [140] M. Jakobsson and M. Yung. “On Assurance Structures for WWW Commerce,” In *Financial Cryptography ’98*. LNCS 1465. Springer-Verlag, 1998. pp. 141–157.
- [141] E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer. “Curbing Junk E-Mail via Secure Classification,” In *Financial Cryptography ’98*. LNCS 1465. Springer-Verlag, 1998. pp. 198–213.
- [142] M. Jakobsson and M. Yung. “Distributed ‘Magic Ink’ Signatures,” In *Advances in Cryptology – EuroCrypt ’97*. LNCS 1233. Springer-Verlag, 1997. pp. 450–464.
- [143] M. Jakobsson and M. Yung. “Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System,” In *Financial Cryptography ’97*. LNCS 1318. Springer-Verlag, 1997. pp. 217–238.
- [144] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. “Proactive public-key and signature schemes,” In *Proceedings of the 4th Annual Conference on Computer Communications Security*. ACM Press, 1997. pp. 100–110.

- [145] M. Bellare, M. Jakobsson, and M. Yung. “Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function,” In Advances in Cryptology – EuroCrypt ’97. LNCS 1233. Springer-Verlag, 1997. pp. 280–305.
- [146] M. Jakobsson and M. Yung. “Proving Without Knowing,” In Crypto ’96. LNCS 1109. Springer-Verlag, 1996. pp. 186–200.
- [147] M. Jakobsson, K. Sako, and R. Impagliazzo. “Designated Verifier Proofs and Their Applications,” In Advances in Cryptology – EuroCrypt ’96. LNCS 1070. Springer-Verlag, 1996. pp. 143–154.
- [148] M. Jakobsson and M. Yung. “Revokable and Versatile Electronic Money,” In CCS ’96: Proceedings of the 3rd ACM conference on Computer and communications security. ACM Press, 1996. pp. 76–87.
- [149] M. Jakobsson. “Ripping Coins for a Fair Exchange,” In Advances in Cryptology – EuroCrypt ’95. LNCS 921. Springer-Verlag, 1995. pp. 220–230.
- [150] M. Jakobsson. “Blackmailing using Undeniable Signatures,” In Advances in Cryptology EuroCrypt ’94. LNCS 950. Springer-Verlag, 1994. pp. 425–427.
- [151] M. Jakobsson. “Reducing costs in identification protocols,” Crypto ’92, 1992.
- [152] M. Jakobsson. “Machine-Generated Music with Themes,” In International Conference on Artificial Neural Networks ’92. Vol 2. Amsterdam: Elsevier, 1992. pp. 1645–1646
- [153] M. Jakobsson, “Social Engineering 2.0: What’s Next,” McAfee Security Journal, Fall 2008
- [154] M. Jakobsson and S. Myers, “Delayed Password Disclosure,” ACM SIGACT News archive, Volume 38, Issue 3 (September 2007), pp. 56 - 75
- [155] V. Griffith and M. Jakobsson. “Messin’ with Texas, Deriving Mother’s Maiden Names Using Public Records,” CryptoBytes, 2007.
- [156] M. Jakobsson, A. Juels, J. Ratkiewicz, “Remote-Harm Detection,” Beta-version available at [rhd.ravenwhitedevelopment.com/](http://rhd.ravenwhitedevelopment.com/)
- [157] S. Stamm, M. Jakobsson, “Social Malware,” Experimental results available at [www.indiana.edu/~phishing/verybigad/](http://www.indiana.edu/~phishing/verybigad/)
- [158] M. Jakobsson. “Privacy vs. Authenticity,” Ph.D. Thesis, University of California at San Diego, 1997
- [159] Markus Jakobsson, Automatic PIN creation using passwords, US20130125214 A1, 2012.

- [160] Markus Jakobsson, Systems and methods for creating a user credential and authentication using the created user credential, US 20130111571 A1, 2012.
- [161] Markus Jakobsson, Password check by decomposing password, US 20120284783 A1, 2012.
- [162] Markus Jakobsson, William Leddy, System and methods for protecting users from malicious content, US 20120192277 A1, 2011.
- [163] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8370935 B1, 2011.
- [164] Markus Jakobsson, Methods and Apparatus for Efficient Computation of One-Way Chains in Cryptographic Applications, US20120303969 A1, 2011.
- [165] Markus Jakobsson, Automatic PIN creation using password, US 20120110634 A1, 2011.
- [166] Markus Jakobsson, Jim Roy Palmer, Gustavo Maldonado, Interactive CAPTCHA, US20130007875 A1, 2011.
- [167] Markus Jakobsson, System access determination based on classification of stimuli, US 20110314559 A1, 2011.
- [168] Markus Jakobsson, System access determination based on classification of stimuli, WO 2011159356 A1, 2011.
- [169] Markus Jakobsson, Method, medium, and system for reducing fraud by increasing guilt during a purchase transaction, US8458041 B1, 2011.
- [170] Markus Jakobsson, Visualization of Access Information, US 20120233314 A1, 2011.
- [171] Markus Jakobsson, Richard Chow, Runting Shi, Implicit authentication, US20120137340 A1, 2010.
- [172] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, EP2467793 A1, 2010.
- [173] Markus Jakobsson, Event log authentication using secure components, US 20110314297 A1, 2010.
- [174] Markus Jakobsson, Philippe J.P. Golle, Risk-based alerts, US 20110314426 A1, 2010.
- [175] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041178 A1, 2010.
- [176] M. Jakobsson, A. Juels, J. Kaliski Jr, S. Burton and others, Identity authentication system and method, US Patent 7,502,933, 2009.

- [177] Markus Jakobsson, Method and system for facilitating throttling of interpolation-based authentication, US8219810 B2, 2009.
- [178] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8375442 B2, 2009.
- [179] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041180 A1, 2009.
- [180] Markus Jakobsson, Pattern-based application classification, US 20110055925 A1, 2009.
- [181] Markus Jakobsson, Method and apparatus for detecting cyber threats, US8286225 B2, 2009.
- [182] Markus Jakobsson, Method and apparatus for detecting cyber threats, US20110035784 A1, 2009.
- [183] Markus Jakobsson, CAPTCHA-free throttling, US8312073 B2, 2009.
- [184] Markus Jakobsson, Captcha-free throttling, US 20110035505 A1, 2009.
- [185] Markus Jakobsson, Christopher Soghoian, Method and apparatus for throttling access using small payments, US 20100153275 A1, 2008.
- [186] Markus Jakobsson, Christopher Soghoian, Method and apparatus for mutual authentication using small payments, US 20100153274 A1, 2008.
- [187] Philippe J.P. Golle, Markus Jakobsson, Richard Chow, Resetting a forgotten password using the password itself as authentication, US 20100125906 A1, 2008.
- [188] Philippe J. P. Golle, Markus Jakobsson, Richard Chow, Authenticating users with memorable personal questions, US8161534 B2, 2008.
- [189] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Authentication based on user behavior, US20100122329 A1, 2008.
- [190] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Enterprise password reset, US 20100122340 A1, 2008.
- [191] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US8086866 B2, 2008.
- [192] Richard Chow, Philippe J. P. Golle, Markus Jakobsson, Selectable captchas, US8307407 B2, 2008.
- [193] Markus Jakobsson, Ari Juels, Sidney Louis Stamm, Method and apparatus for combatting click fraud, US 20080162227 A1, 2007.
- [194] Jakobsson, Method and apparatus for evaluating actions performed on a client device, US 20080037791 A1, 2007.

- [195] Jakobsson, Ari Juels, Method and apparatus for storing information in a browser storage area of a client device, US 20070106748 A1, 2006.
- [196] Markus Jakobsson, Steven Andrew Myers, Anti-phising logon authentication object oriented system and method, WO 2006062838 A1, 2005.
- [197] Jakobsson, Jean-Pierre Hubaux,Levente Buttyan, Micro-payment scheme encouraging collaboration in multi-hop cellular networks, US 20050165696 A1, 2004.
- [198] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , System and method providing disconnected authentication, WO2005029746 A3, 2004.
- [199] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane Rice, Ronald Rivest, Less , System and method providing disconnected authentication, US 20050166263 A1, 2004.
- [200] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , Systeme et procede d'authentification deconnectee, WO 2005029746 A2, 2004.
- [201] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Identity authentication system and method, WO2004051585 A3, 2003.
- [202] Markus Jakobsson, Ari Juels, Burton S. Kaliski, Jr., Identity authentication system and method, US 7502933 B2, 2003.
- [203] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Systeme et procede de validation d'identite, WO 2004051585 A2, 2003.
- [204] Markus Jakobsson, Burton S. Kaliski, Jr., Method and apparatus for graph-based partition of cryptographic functionality, US7730518 B2, 2003.
- [205] Markus Jakobsson, Phong Q. Nguyen, Methods and apparatus for private certificates in public key cryptography, US7404078 B2, 2002.
- [206] Jakobsson, Philip MacKenzie, Thomas Shrimpton, Method and apparatus for performing multi-server threshold password-authenticated key exchange, US20030221102 A1, 2002.
- [207] Markus Jakobsson, Philip D MacKenzie, Method and apparatus for distributing shares of a password for use in multi-server password authentication, US 7073068 B2, 2002.
- [208] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, EP 1389376 A1 (text from WO2002084944A1), 2002.

- [209] Markus Jakobsson, Adam Lucas Young, Method and apparatus for identification tagging documents in a computer system, US 7356845 B2, 2002.
- [210] Juan A. Garay, Markus Jakobsson, Methods and apparatus for computationally-efficient generation of secure digital signatures, US 7366911 B2, 2001.
- [211] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US 7404080 B2, 2001.
- [212] Markus Jakobsson, Susanne Gudrun Wetzel, Securing the identity of a bluetooth master device (bd addr) against eavesdropping by preventing the association of a detected channel access code (cac) with the identity of a particular bluetooth device, WO2002019641 A3, 2001.
- [213] Markus Jakobsson, Susanne Gudrun Wetzel, Procede et appareil permettant d'assurer la securite d'utilisateurs de dispositifs a capacites bluetooth, WO 2002019641 A2, 2001.
- [214] Robert M. Arlein, Ben Jai, Markus Jakobsson, Fabian Monroe, Michael Kendrick Reiter, Less , Methods and apparatus for providing privacy-preserving global customization, US 7107269 B2, 2001.
- [215] Markus Jakobsson, Susanne Gudrun Wetzel, Secure distributed computation in cryptographic applications, US6950937 B2, 2001.
- [216] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of short range wireless enable devices, US6981157 B2, 2001.
- [217] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of bluetooth TM-enabled devices, US 6574455 B2, 2001.
- [218] Garay; Juan A. (West New York, NJ), Jakobsson; M. (Hoboken, NJ), Kristol; David M. (Summit, NJ), Mizikovsky; Semyon B.(Morganville, NJ), Cryptographic key processing and storage , 7023998, 2001.
- [219] Markus Jakobsson, Method, apparatus, and article of manufacture for generating secure recommendations from market-based financial instrument prices, US 6970839 B2, 2001.
- [220] Markus Jakobsson, Encryption method and apparatus with escrow guarantees, US7035403 B2, 2001.
- [221] Jakobsson, Call originator access control through user-specified pricing mechanism in a communication network, US20020099670 A1, 2001.
- [222] Markus Jakobsson, Claus Peter Schnorr, Tagged private information retrieval, US7013295 B2, 2000.

- [223] Markus Jakobsson, Secure enclosure for key exchange, US 7065655 B1, 2000.
- [224] Markus Jakobsson, Michael Kendrick Reiter, Software aging method and apparatus for discouraging software piracy, US 7003110 B1, 2000.
- [225] Markus Jakobsson, Probabilistic theft deterrence, US6501380 B1, 2000.
- [226] Markus Jakobsson, Michael Kendrick Reiter, Abraham Silberschatz, Anonymous and secure electronic commerce, EP 1150227 A1, 2000.
- [227] Markus Jakobsson, Ari Juels, Proofs of work and bread pudding protocols, US 7356696 B1, 2000.
- [228] Markus Jakobsson, Joy Colette Mueller, Methods of protecting against spam electronic mail, US7644274 B1, 2000.
- [229] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, EP1043862 B1, 2000.
- [230] Markus Jakobsson, Ari Juels, Mix and match: a new approach to secure multiparty computation, US6772339 B1, 2000.
- [231] Markus Jakobsson, Ari Juels, Mixing in small batches, US6813354 B1, 2000.
- [232] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, US 6901145 B1, 36566
- [233] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US6931126 B1, 2000.
- [234] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US 6931126 B1, 2000.
- [235] Markus Jakobsson, Flash mixing apparatus and method, US 6598163 B1, 1999.
- [236] Markus Jakobsson, Minimalistic electronic commerce system, US 6529884 B1, 1999.
- [237] Markus Jakobsson, Method and system for providing translation certificates, US 6687822 B1, 1999.
- [238] Markus Jakobsson, Verification of correct exponentiation or other operations in cryptographic applications, US6978372 B1, 1999.

- [239] Markus Jakobsson, Non malleable encryption apparatus and method, US 6507656 B1, 1999.
- [240] Markus Jakobsson, Method and system for quorum controlled asymmetric proxy encryption, US 6587946 B1, 1998.
- [241] Markus Jakobsson, Practical mix-based election scheme, US 6317833 B1, 1998.
- [242] Markus Jakobsson, Ari Juels, Method and apparatus for extracting unbiased random bits from a potentially biased source of randomness, US 6393447 B1, 1998.
- [243] Markus Jakobsson, Ari Juels, Executable digital cash for electronic commerce, US6157920 A, 1998.
- [244] Bruce Kenneth Hillyer, Markus Jakobsson, Elizabeth Shriver, Storage device random bit generator, US 6317499 B1, 1998.
- [245] Markus Jakobsson, Method and apparatus for encrypting, decrypting, and providing privacy for data values, US 6049613 A, 1998.